

REMARKS/ARGUMENTS

This Amendment is being filed in response to the first Official Action on a second Request for Continued Examination (RCE) for the present application. The first Official Action of this second RCE no longer rejects any of the pending claims, namely Claims 1-20, under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,330,562 to Boden et al. Instead, the Official Action adds U.S. Patent No. 7,107,464 to Shapira et al., and rejects all of the pending claims as being unpatentable over Boden, in view of Shapira. That is, the Official Action rejects Claims 1-20 under 35 U.S.C. § 103(a) as being unpatentable over Boden, in view of Sharpira. Applicant does note, however, that the Official Action formally rejects all of the pending claims under 35 U.S.C. § 102(b) as being anticipated by Boden, in view of Sharpira. This indication appears to be a typographical error, however, as the Official Action fails to support an anticipation rejection of any of the pending claims; such a rejection requiring a single reference that discloses every element of the claimed invention.

As explained below, Applicant respectfully submits that the claimed invention is patentably distinct from Boden and Shapira, taken individually or in any proper combination, and accordingly, traverses the respective objection to the drawings and rejection of the claims. Nonetheless, Applicant has amended various ones of the claims to further clarify the claimed invention. In view of the amendments to the claims and the remarks presented herein, Applicant respectfully requests reconsideration and allowance of all of the pending claims of the present application.

A. Claims 1-5 and 11-20 are Patentable

As currently recited by amended independent Claim 1, for example, a method of creating and maintaining a centralized key store includes providing a plurality of security policies to be applied to traffic to and/or from a host, each of which includes an application instance identifier identifying a security service. As recited, at least two of the application instance identifiers identify different security services that provide security to packets of data according to different protocols at different layers of a multi-layered protocol stack. As also recited, the method further includes creating a plurality of security associations in accordance with the security services

identified by the application instance identifiers. At least two security associations are created based upon respective ones of the different security services to thereby create a centralized key store including the plurality of security policies and security associations, and at least one of the security associations is created according to a key management protocol that differs from the protocols according to which the security services provide security.

1. Security Policies

In contrast to amended independent Claim 1, neither Boden nor Shapira, taken individually or in any proper combination, teaches or suggests a centralized key store with security policies at least two of which include application instance identifiers identifying different, independent security services that provide security to packets of data. The Official Action notes that that Boden discloses IKE and IPSec, and asserts that IKE and IPSec are security services that operate according to different protocols at different layers of a multi-layered protocol stack. In addition, the Official Action appears to interpret key management security policies (see FIG. 3, policies 36) and data management security policies (see FIG. 3, policies 58) as corresponding to policies associated with different security services, namely IKE and IPSec. To the contrary, however, Applicant notes that IKE is not a security service as is IPSec. That is, IKE is not a security service that provides security to packets of data as do the different security services of amended independent Claim 1, but is instead a key management protocol for creating security associations for use in implementing IPSec. Moreover, IKE and IPSec are not independent security services as are the different security services of amended independent Claim 1, but instead operate in concert with one another to implement the IPSec security service.

2. Security Associations

Also in contrast to amended independent Claim 1, neither Boden nor Shapira, taken individually or in any proper combination, teaches or suggests creating security associations at least two of which are created in accordance with respective ones of different security services. The Official Action cites a passage of Boden disclosing use of IKE to create security

associations (SA). But this passage still does not support creating two or more security associations in accordance with different security services. One could argue that Boden discloses creating a security association in accordance with IKE, or because IKE creates security associations for use in IPSec, creating a security association in accordance with IPSec. But even in this instance (following solely for the sake of argument the interpretation of security services proffered in the Official Action), Boden still does not teach or suggest creating two or more security associations in accordance with respective ones of the different security services, similar to amended independent Claim 1. Instead, in either interpretation, Boden discloses creating its security associations in accordance with IPSec (directly or by extension by IKE).

3. Key Management Protocol

Relative to former independent Claim 1, the Official Action states that Boden does not teach or suggest creating a security association according to a key management protocol that differs from the protocols according to which the security services operate (now reciting according to which the security services “provide security”). Instead, the Official Action cites Shapira for this feature, and alleges that one skilled in the art would have been motivated to modify Boden per this feature of Shapira. Applicant respectfully disagrees.

Contrary to the assertions of the Official Action, Boden does in fact disclose a key management protocol (i.e., IKE) for creating security associations in accordance with a security service (i.e., IPSec), and that differs from protocols according to which security services (e.g., IPSec) provide security. Again, however, Boden does not teach or suggest a plurality of policies including application instance identifiers at least two of which identify different, independent security services, as recited by amended independent Claim 1. And for at least the reason that the recited key management protocol differs from the protocols according to which the security services provide security, IKE cannot be considered a security service, as alleged in the Official Action.

4. Insufficient Reasoning for Combination

Moreover, Applicant respectfully submits that the Official Action fails to provide any

sufficient reasoning for the combination of Boden and Shapira in the manner alleged. Applicant acknowledges the Supreme Court's recent decision in which the Court rejected a rigid application of the "teaching, suggestion or motivation" (TSM) test. *KSR Int'l. Co. v. Teleflex, Inc.*, 127 S.Ct. 1727, 82 USPQ2d (BNA) 1385 (2007). Nonetheless, in *KSR Int'l. Co.*, the Court did state that obviousness often requires determining whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue, and that to facilitate review, this analysis should be made explicit. See *KSR Int'l. Co.*, 127 S.Ct. at 1740-41, 82 USPQ2d (BNA) at 1396. Even further, the Court noted that "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements"; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.*, 127 S.Ct. at 1740-41, 82 USPQ2d (BNA) at 1396, citing *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d (BNA) 1329 (Fed. Cir. 2006) (emphasis added).

As clearly explained by the Supreme Court in *KSR Int'l. Co.*, then, any finding of obviousness should be based on an apparent reason to combine the prior art, and must be supported by more than mere conclusory statements. In the instant case, the Official Action attempts to support the alleged combination of Andric and Kredo by merely asserting that one skilled in the art would have been "motivated by the advantages of a more useful system (i.e. the ability to provision more security services) to modify Boden to include the feature of Shapira. Official Action of Feb. 6, 2008, page 4. However, the Examiner fails to cite any evidence to support this assertion.

Applicant therefore respectfully submits that amended independent Claim 1, and by dependency Claims 2-5, are patentably distinct from Boden and Shapira, taken individually or in any proper combination. Applicant also respectfully submits that amended independent Claims 11 and 16 recite subject matter similar to that of amended independent Claim 1, including the aforementioned centralized key store, and application with at least one security association created according to a key management protocol that differs from the protocols according to which the security services operate. Applicant therefore respectfully submits that amended independent Claims 11 and 16, and by dependency Claims 12-15 and 17-20, are also patentably distinct from Boden and Shapira, taken individually or in any proper combination, for at least the

reasons given above with respect to amended independent Claim 1.

For at least the foregoing reasons, Applicant respectfully submits that the rejection of Claims 1-5 and 11-20 as being unpatentable over Boden, in view of Shapiro is overcome.

B. Claims 6-10 are Patentable

Amended independent Claim 6 recites an apparatus including a processor configured to provide a plurality of security policies to be applied to traffic to and/or from the apparatus. Similar to amended independent Claims 1, 11 and 16, each of the security policies includes an application instance identifier identifying a security service, and at least two of the application instance identifiers identify different security services that provide security to packets according to different, independent protocols at different layers of a multi-layered protocol stack. As also recited, the processor is configured to apply the security services identified by respective, identified application instance identifiers to packets of data, including being configured to apply different security services to at least two different packets of data, to thereby transform the packets of data. In this regard, the processor is configured to apply the security services to the packets based upon the plurality of security policies and a plurality of security associations. The processor, then, is configured to relay the transformed packets of data to one or more security gateways configured to apply the security services identified by the respective, identified application instance identifiers to the transformed packets of data to thereby generate representations of the respective packets of data.

As indicated above and previously explained, neither Boden nor Shapira, taken individually or in any proper combination, teaches or suggests security policies at least two of which include application instance identifiers identifying different, independent security services that provide security to packets of data, as recited by amended independent Claim 1 and similarly independent Claim 6. Moreover, the Official Action fails to provide any sufficient reasoning for the combination of Boden and Shapira in the manner alleged. Again noting that the Official Action appears to interpret IKE and IPSec to correspond to the recited security services, even considering this interpretation, Boden still does not teach or suggest applying different security services to at least two different packets of data based upon security policies and security

Appl. No.: 10/608,690
Amdt. dated August 6, 2008
Reply to Official Action of February 6, 2008

associations to thereby transform the packets of data. As indicated above, even if IKE were generally interpreted as a security service, IKE is not applied to any packet of data based upon any security policy and security association to transform the packet. Rather, IKE is a key management protocol for creating security associations for use in implementing IPSec.

For at least the foregoing reasons, as well as those presented above with respect to amended independent Claim 1, Applicant respectfully submits that amended independent Claim 6, and by dependency Claims 7-10, is also patentably distinct from Boden. And as such, Applicant respectfully submits that the rejection of Claims 6-10 as being anticipated by Boden is overcome.

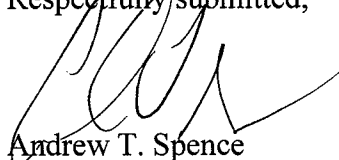
Appl. No.: 10/608,690
Amdt. dated August 6, 2008
Reply to Official Action of February 6, 2008

CONCLUSION

In view of the amendments to the claims and the remarks presented above, Applicant respectfully submits that the present application is in condition for allowance. As such, the issuance of a Notice of Allowance is therefore respectfully requested. In order to expedite the examination of the present application, the Examiner is encouraged to contact Applicant's undersigned attorney in order to resolve any remaining issues.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,



Andrew T. Spence
Registration No. 45,699

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111
LEGAL02/30887317v1

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON AUGUST 6, 2008.